

AMENDMENTS TO THE CLAIMS

1-18. (Canceled)

19. (New) A password recovery system for re-supplying a password to a user who has forgotten the password, said password recovery system comprising:

a communication terminal device; and

a portable password recording medium having the password recorded thereon and being coupled to said communication terminal device,

wherein said communication terminal device comprises:

a first receiving unit operable to receive, from an external communication terminal device, a signed data set generated by digitally signing information for identifying a sender with use of a secret key; and

an outputting unit operable to output the signed data set received by said first receiving unit to said password recording medium, and

wherein said password recording medium comprises:

a public key storing unit for storing therein a public key generated with use of the secret key;

a password storing unit for storing the password therein;

a second receiving unit operable to receive the signed data set output by said outputting unit;

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said second receiving unit so as to judge if the signed data set received by said

second receiving unit has been generated by the sender; and

a reading unit operable, when said authentication unit judges that the signed data set received by said second receiving unit has been generated by the sender, to read the password from said password storing unit.

20. (New) The password recovery system of claim 19,

wherein said password recording medium further comprises an expiration period storing unit for storing therein an expiration period for receiving the signed data set,

wherein the signed data set received by said second receiving unit has date/time information attached thereto, the date/time information indicating a date and time at which the signed data set has been generated,

wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said second receiving unit has been generated by the sender, and judges if the date/time information attached to the signed data set is within the expiration period stored in said expiration period storing unit, and

wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the received signed data set has been generated by the sender and that the date/time information is within the expiration period.

21. (New) The password recovery system of claim 19,

wherein said password recording medium further comprises a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data

sets that are required for performing a password recovery, and

wherein said reading unit counts the received signed data set as a valid signed data set for performing the password recovery when said authentication unit judges that the signed data set received by said second receiving unit has been generated by the sender, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit.

22. (New) A communication terminal device for re-supplying a password to a user who has forgotten the password, said communication terminal comprising:

a public key storing unit for storing therein a public key generated with use of a secret key;

a password storing unit for storing the password therein;

a receiving unit operable to receive, from an external communication terminal device, a signed data set generated by digitally signing information for identifying a sender with use of a secret key;

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said receiving unit so as to judge if the signed data set received by said receiving unit has been generated by the sender; and

a reading unit operable, when said authentication unit judges that the signed data set received by said receiving unit has been generated by the sender, to read the password from said password storing unit.

23. (New) The communication terminal device of claim 22, further comprising an expiration period storing unit for storing therein an expiration period for receiving the signed data set,

wherein the signed data set received by said receiving unit has date/time information attached thereto, the date/time information indicating a date and time at which the signed data set has been generated,

wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said receiving unit has been generated by the sender, and judges if the date/time information attached to the signed data set is within the expiration period stored in the expiration period storing unit, and

wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the signed data set received by said receiving unit has been generated by the sender and that the date/time information is within the expiration period.

24. (New) The communication terminal device of claim 22, further comprising a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data sets that are required for performing a password recovery,

wherein said reading unit counts the received signed data set as a valid signed data set for performing the password recovery when said authentication unit judges that the received signed data set has been generated by the sender, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit.

25. (New) The communication terminal device of claim 22, further comprising a displaying unit operable to display the password read by said reading unit.

26. (New) The communication terminal device of claim 22, further comprising:
an application storing unit for storing therein a piece of application software that corresponds to the password; and
an application executing unit operable to execute the piece of application software, using the password read by said reading unit.

27. (New) A password recording medium that is portable and operable to re-supply a password to a user who has forgotten the password, said password recording medium comprising:

a public key storing unit for storing therein a public key generated with use of a secret key;

a password storing unit for storing the password therein;

a receiving unit operable to receive, from a communication terminal device to which said password recording medium is coupled, a signed data set generated by digitally signing information for identifying a sender with use of a secret key;

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said receiving unit so as to judge if the signed data set received by said receiving unit has been generated by the sender; and

a reading unit operable, when said authentication unit judges that the signed data set received by said receiving unit has been generated by the sender, to read the password from said password storing unit.

28. (New) The password recording medium of claim 27, further comprising an expiration period storing unit for storing therein an expiration period for receiving the signed data set,

wherein the signed data set received by said receiving unit has date/time information attached thereto, the date/time information indicating a date and time at which the signed data set has been generated,

wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said receiving unit has been generated by the sender, and judges if the date/time information attached to the signed data set is within the expiration period stored in said expiration period storing unit, and

wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the signed data set received by said receiving unit has been generated by the sender and that the date/time information is within the expiration period.

29. (New) The password recording medium of Claim 27, further comprising a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data sets required for performing a password recovery, wherein said reading unit counts the received signed data set as a valid signed data set

for performing the password recovery when said authentication unit judges that the received signed data set has been generated by the sender, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit.

30. (New) The password recording medium of claim 27, further comprising
an outputting unit operable to output the password read by said reading unit to the communication terminal device.

31. (New) The password recording medium of claim 27, further comprising:
an application storing unit for storing therein a piece of application software that corresponds to the password; and
an application executing unit operable to execute the piece of application software, using the password read by said reading unit.

32. (New) A password recovery method to be used by a password recording medium that is portable and operable to re-supply a password to a user who has forgotten the password,

the password recording medium comprising:
a public key storing unit for storing therein a public key generated with use of a secret key; and
a password storing unit for storing the password therein, and

the password recovery method comprising:

a receiving step of receiving a signed data set generated by digitally signing information for identifying a sender with use of a secret key;

an authentication step of reading the public key from the public key storing unit and performing signature authentication using the read public key and the signed data set so as to judge if the received signed data set has been generated by the sender; and

a reading step of, when the authentication step judges that the signed data set has been generated by the sender, reading the password from the password storing unit.

33. (New) A computer-readable storage medium on which a password recovery program is recorded for execution within a computer, the password recovery program being used by a password recording medium that is portable and operable to perform a password recovery method of re-supplying a password to a user who has forgotten the password,

the password recording medium comprising:

a public key storing unit for storing therein a public key generated with use of a secret key; and

a password storing unit for storing the password therein, and

the password recovery method comprising:

a receiving step of receiving a signed data set generated by digitally signing information for identifying a sender with use of a secret key;

an authentication step of reading the public key from the public key storing unit and performing signature authentication using the read public key and the signed data set so as to

judge if the received signed data set has been generated by the sender; and

a reading step of, when the authentication step judges that the signed data set has been generated by the sender, reading the password from the password storing unit.